UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,621	10/30/2003	Makoto Fujiwara	60188-694	5601

7590 01/23/2008

Jack Q. Lever, Jr.
McDERMOTT, WILL & EMERY
600 Thirteenth Street, N.W.
Washington, DC 20005-3096

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
01/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MW

Office Action Summary	Application No.	Applicant(s)	
	10/696,621	FUJIWARA ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 10/30/2007, applicant has amended claim 1 to incorporate the limitations of claim 9 previously withdrawn; upon further consideration the requirement for restriction is withdrawn and groups I and II have been rejoined. Claims 1-11 are pending.

1.1 In response to communications filed on 10/30/2007, the double patenting rejection has been withdrawn with respect to the amendment.

1.2 Applicant's arguments, see pages 6-9, filed on 10/30/2007, with respect to the -- rejection(s) of claim(s) 1-8 have been fully considered but they are not persuasive as amended. Applicant argues that Rindsberg does not disclose the added limitations. However, applicant has not shown how the language of claim 1 as amended patentably distinguishes it from the other references such as Etzel reference. Applicant has amended the claims to more particularly point out the invention, upon further consideration, a new ground of rejection is made. The rejection of the other claims not challenged by Applicant can still be applied. The rejection of claims 1-11 is set forth below.

Double Patenting

2. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and

useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

Claims 9-11 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 9-11 of copending Application No. 11/798,367. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 recites 3 steps as amended and further recites a first step... second step... third step..., it is not clear whether the three steps recited at the beginning are intended to be part

of preamble and/or what makes the receiving step a first step. Appropriate correction is requested. Claim 9 recites determining whether a program is transmitted and if it is determined that the program is transmitted, transmitting the program. It appears that the claim is reciting transmitting something that is known as being already transmitted. Appropriate correction is required. For purpose of examination, Examiner will interpret the claim as the program is not already transmitted at the second step.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 and 8 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 7,110,984 to **Spagna et al.**

As per claim 1, **Spagna et al** discloses a method for updating an inherent key-encrypted program in a system including an LSI device and an external memory, the inherent

key-encrypted program being generated by encryption with an inherent key unique to the LSI device and being stored in the external memory, the method comprising:

Spagna et al discloses transmitting by the system to a server (the server is not limited to any of the elements as shown in fig.1 see also column 20, line 129 through column 21, line 130) identification information that includes a content ID, application ID, user information which includes user device ID (see column 48, lines 16-40 and column 26, lines 25-35) that meets the recitation of a step of *transmitting by the system an ID of the LSI device and an application ID which is identification information of an update object program to a server*;

Spagna et al discloses the server verifies whether or not program requested by the user should be transmitted based on the transmitted identification information (such as license information) and further discloses transmitted by the server additional information if it is determined that the update obiect program may be transmitted (see column 26, lines 36-55 and column 39, lines 49-67) that meets the recitation of *a step of determining by the server whether or not the update object program may be transmitted based on the transmitted ID and application ID, and transmitting by the server additional information of the update object program if it is determined that the update obiect program may be transmitted*; **Spagna et al** discloses a step of determining by the system if program update is possible based on transmitted additional information (see column 45, lines 48-51) and further discloses requesting by the system to the server to transmit common-key encrypted content generated by encryption with a common key if it is determined that program update is possible (see column 30, lines 20-30) that meets the recitation of *a step of determining by the system whether or not program update is possible based on the transmitted additional information, and requesting by the system to the server to transmit a common key-*

encrypted program generated by encryption with a common key if it is determined that program update is possible; **Spagna et al** discloses *receiving by the system a common key-encrypted program generated by encryption with a common key and transmitted from the server* (see column 30, lines 20-30); **Spagna et al** discloses *a second step of decrypting by the system the received common key- encrypted program to generate a raw program* (see column 30, lines 20-30). **Spagna et al** discloses *re-encrypting by the system the raw program with the inherent key and storing the re-encrypted program in the external memory as a new inherent key-encrypted program* (see column 91, lines 44-61) and also discloses in column 95, lines 63-67 the option of using an external memory for storage.

As per claim 8, **Spagna et al** discloses receiving a hash value of the raw program transmitted from the server and the received hash value is used to perform a hash verification on the decrypted raw program (see column 41, line 49 through column 42, line 19).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 4, 6, 7, and 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 7,110,984 to **Spagna et al** in view of US Patent 6,577,734 to **Etzel et al**.

As per claim 2, **Spagna et al** substantially teaches the claimed method of claim 1. **Spagna et al** is silent about receiving by the system common key information transmitted from the server and generating by the system a raw common key using the received common key information. **Etzel et al** in an analogous art discloses receiving by a device shared key information transmitted from system 100 and generating a shared key using the shared key information (see column 6, lines 6-20) that meets the recitation of receiving by the system common key information transmitted from the server and generating by the system a raw common key using the received common key information and further discloses wherein at the second step, the raw common key is used to decrypt the common key-encrypted program (see column 7, lines 39-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Spagna et al** to allow each device to generate own shared key from common key information as taught by **Etzel et al** because it would avoid transmission and/or storing of the key and thereby preventing the key to be obtained by unauthorized party as suggested by **Spagna et al** (see **Spagna et al**, column 91, lines 44-53).

As per claim 4, **Spagna et al** discloses generating the key at startup and storing inherent key information in the internal memory (see column 88, lines 49-63), but does not explicitly state the system uses the inherent key information stored in the internal memory to generate a raw inherent key at boot-up of the system. **Etzel et al** in an analogous art discloses during booting

generating a unique device key using device key information and stored in its secure memory to prevent tampering (see column 3, lines 12-36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rindsberg** to allow each device to generate unique device key upon startup using inherent key information as taught by **Etzel et al** so as to securely manage the keys and prevent them from being misappropriated for fraudulent purposes (see **Etzel et al,** column 1, lines 47-50).

As per claim 6, the combination of **Spagna et al** and **Etzel et al** discloses wherein the generated raw inherent key is stored in a register of the LSI device and is used for decrypting the inherent key-encrypted program to a raw program for execution of the inherent key-encrypted program (see **Spagna**, column 39, lines 22-25 and column 30, lines 20-30).

As per claim 7, the combination of **Spagna et al** and **Etzel et al** discloses the LSI device includes a boot ROM in which a boot program is stored (see **Etzel et al**, column 9, lines 20-34); **Spagna et al** discloses external memory interface and additional interfaces or communication link and receiver for establishing data transmission with the server (see column 61, lines 24-67) that meets the recitation of external memory includes an acquisition program for establishing data transmission between the LSI device and a server; **Etzel et al** also discloses controlling update processing performed after the reception of the common key-encrypted program based on the boot program stored in the boot ROM (see **Etzel et al**, column 9, lines 20-30 and lines 50-63). Claim 7 is therefore rejected on the same rationale as the rejection of claim 2 above.

As per claim 9, **Spagna et al** substantially discloses a server which operates for program update in a system including an LSI device, the server executing receiving from the system by a server (the server is not limited to any of the elements as shown in fig.1 see also column 20, line 129 through column 21, line 130) identification information that includes a content ID, application ID, user information which includes user device ID (see column 48, lines 16-40 and column 26, lines 25-35) that meets the recitation of a step of *a first step of receiving from the system an ID of the LSI device and an application ID which is identification information of an update object program;* **Spagna et al** discloses verifying whether or not program requested by the user should be transmitted based on the transmitted identification information (such as license information) (see column 26, lines 36-55); **Spagna et al** discloses transmitted by the server additional information if it is determined that the update object program may be transmitted (see column 26, lines 36-55 and column 39, lines 49-67) and further discloses transmitting common-key encrypted content generated by encryption with a common key (see column 30, lines 1-30) and common key information from which the common key is derived (see column 44, lines 4-27) that meets the recitation of, *if it is determined at the second step that the update object program is transmitted to the system, a third step of transmitting to the system a common key-encrypted program generated by encrypting the update object program with a common key and common key information from which the common key is derived.*

Spagna et al is silent about *referring a first table which indicates correspondences between application IDs and LSI IDs* **Etzel et al** in an analogous art discloses the server stores the encrypted program in association with the serial number and the program identifier (see column 2, line 61 through column 3, line 3) one of ordinary skill in the art understands that it

would make sense to determine that there is a match between the device and the program identifiers before transmitting the program (see for instance fig. 2 and column 8, lines 20-25); Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Spagna et al** to use a table which indicates correspondences between application IDs and LSI ID*s* as taught by **Etzel et al** because it would help in making decision about the validity of the request as suggested by **Etzel et al** (see column 8, lines 24-26).

As per claim 10, **Spagna et al** discloses logging application information and device ID necessary for execution of the update object program and receiving from the system a signal which requests application inherent information necessary for execution of the update object program (see column 26, lines 25-55) and determining whether or not the application inherent information requested at the fourth step is transmitted using the log and record (see column 41, line 49 through column 42, line 20 and lines 20 and seq.) that meets the recitation of a fourth step of receiving from the system a signal which requests application inherent information necessary for execution of the update object program and a fifth step of referring to a second table which indicates correspondence between a transmission history of the application inherent information and the LSI IDs to determine whether or not the application inherent information requested at the fourth step is transmitted.

6. **Claims 3, 5,** and **11** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 7,110,984 to **Spagna et al** in view of US Patent 6,577,734 to **Etzel et al** as applied to

claims 1-2 and further in view of US Patent Publication US 2002/0116632 to **Itoh et al** *(Applicant's IDS).*

As per claim 3, the combination of **Spagna et al** and **Etzel et al** discloses the claimed method of claim 2. Neither of the references explicitly discloses double encryption. **Itoh et al** in an analogous art discloses an encrypted common key generated by encrypting software key Ksoft with Ks2 and Ks2 generated by encrypting Ks2 with Ks1 (see page 6, paragraphs 93-95) that meets the recitation of wherein the common key information includes an encrypted common key generated by encrypting the raw common key with a raw first intermediate key, and an encrypted first intermediate key generated by encrypting the raw first intermediate key with a raw second intermediate key. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a double encrypted key as taught by allow each device to generate own shared key from common key information as taught by **Itoh et al** because having the software key dependent on two keys in a double encryption method would make the key less vulnerable against tampering.

As per claim 5, the combination of **Spagna et al** and **Etzel et al** discloses the claimed method of claim 4. Claim 5 is similar to claim 3 except for double encrypting the raw inherent key whereas claim 3 double encrypts the raw common key. **Itoh et al** discloses double encryption as shown in claim 3 above. Therefore, claim 5 is rejected on the same rationale as the rejection of claim 3 above.

As per claim 11, Claim 11 discloses the same limitations as claim 3, therefore, claim 11 is rejected on the same rationale as the rejection of claim 3 above.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the prior art discloses different cryptographic algorithms such as re-encryption and double encryption methods. (See PTO-form 892).

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/

Carl Colin

Patent Examiner, A.U. 2136

January 18, 2008